

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

TOM HAMMOND, WILLIAM H.
WICKS, and LINDA YOUNG, on behalf
of themselves and all others similarly
situated,

Plaintiffs,

vs.

THE BANK OF NEW YORK MELLON
CORPORATION, and JOHN DOES 1-
20,

Defendants.

Civil Action No. **08 CV 6060**
CLASS ACTION
Complaint For Violations of the Michigan
Consumer Protection Act; the Pennsylvania
Unfair Trade Practices and Consumer Protection
Law; the New York General Business Law;
Breach Of Implied Contract; Negligence, Per Se,
and Gross Negligence.
JURY TRIAL DEMANDED

Tom Hammond, William H. Wicks, and Linda Young (collectively, "Plaintiffs"), on
behalf of themselves and all others similarly situated, by and through their attorneys, allege as
follows:

INTRODUCTION

1. This is a class action lawsuit brought on behalf of Plaintiffs, individually, and on
behalf of similarly situated consumers whose names, addresses, Social Security numbers, bank
account information, and/or shareholder account information (the "Sensitive Personal
Information") were accessed and/or compromised by third parties while entrusted to Defendant
The Bank of New York Mellon Corporation ("BNY"). Defendant BNY processes payments on
behalf of its corporate customers, and provides stock transfer, employee plan administration, and
related services for issuers of securities. In connection with these duties, BNY comes into the
possession of – and is entrusted with – the Sensitive Personal Information of millions of
consumers across the United States.

2. In or around February of 2008, a BNY metal box with six to ten unencrypted computer back-up tapes containing the Sensitive Personal Information of consumers was “lost” from a truck operated by Archival Systems, Inc. Archival Systems, Inc., a service provider within the meaning of the Interagency Guidelines Establishing Information Security Standards (the “Security Guidelines”) and the Safeguards Rule issued by the Federal Trade Commission (“FTC”) found at 16 C.F.R. § 314.2(d), pursuant to § 501 *et. seq.* of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et. seq.* (“GLB”), is, upon information and belief, a company selected and used by BNY to transport and store these types of back-up tapes. These “lost” back-up tapes reportedly contained the Sensitive Personal Information of approximately 4.5 million consumers. Upon information and belief, BNY did not begin notifying its customers of this known security breach until mid-April, and is still in the process of notifying all of the consumers whose Sensitive Personal Information has been compromised.

3. When it initially began notifying consumers of the loss of their Sensitive Personal Information, BNY offered affected consumers the opportunity to receive free credit monitoring for a period of 12 months. On or around May 21, 2008 Richard Blumenthal, the Attorney General for the State of Connecticut, sent a letter to BNY’s general counsel addressing the data breach and BNY’s conduct associated therewith. A copy of this letter is attached hereto as Exhibit A. Attorney General Blumenthal described this proposed one year worth of credit monitoring as “grossly inadequate.”

4. Yet another security breach occurred on or around April 29, 2008 again involving the Sensitive Personal Information of consumers that was entrusted to BNY. This time, a back-up data storage tape containing images of scanned checks and other payment documents was “lost” while being transported from Philadelphia to Pittsburgh. It is unknown how many

individual consumers were affected by the second breach, but it has been reported that it involved data from forty-seven (47) institutional clients of BNY. In a letter to consumers, BNY revealed that this second breach “may include Sensitive Personal Information about you, such as name, address and social security number.” A copy of this letter, which was received by Plaintiff Linda Young on or around June 9, 2008, is attached hereto as Exhibit B.

5. Plaintiffs bring this lawsuit for the purpose of securing full, appropriate, and meaningful relief based on Defendants’ negligent, fraudulent, reckless, wrongful and unlawful conduct, to wit:

- a. First, Plaintiffs seek relief based on the injuries suffered by them and members of the Class as a result of Defendants’ failure to provide adequate safeguards to protect its customers’ data, which would have prevented such a widespread security breach from occurring in the first place. Plaintiffs also seek prospective equitable relief to ensure that BNY takes necessary measures to make certain that such massive data breaches do not reoccur in the future.
- b. Second, Plaintiffs seek appropriate relief for Defendants’ inexplicable delays in announcing the security breaches that occurred in February 2008 and April 2008. These unreasonable delays prevented and/or hindered Plaintiffs and members of the Class from taking immediate steps to monitor and attempt to safeguard their financial information. Upon information and belief, Defendant BNY *still* has not notified all of the consumers that had their Sensitive Personal Information compromised in the February 2008 breach.

- c. Third, Plaintiffs seek meaningful and appropriate relief on behalf of themselves and the Class. Defendant BNY's offer to provide affected consumers with free credit monitoring for only two years is wholly inadequate and insufficient.

6. Defendant BNY and the John Doe Defendants' actions constitute violations of the Michigan Consumer Protection Act, the Pennsylvania Unfair Trade Practices and Consumer Protection Law, the New York General Business Law, and amount to a breach of implied contract, negligence *per se*, and gross negligence. Plaintiffs seek monetary damages and other appropriate relief as a result of injuries suffered from Defendants' misconduct.

PARTIES

7. Plaintiff Tom Hammond ("Hammond") is a resident of Auburn Hills, Michigan. In or around May of 2008, Hammond received a letter from Defendant BNY informing him that his Sensitive Personal Information was contained on one of the back-up data tapes that was involved in the February 27, 2008 incident. A true and correct copy of the letter received by Hammond (with his personal activation code redacted), is attached hereto as Exhibit C. As a proximate result of Defendants' conduct alleged herein, Hammond has suffered injuries. Specifically, Hammond's private, nonpublic personal and financial information has been improperly and illegally compromised and/or disseminated to third parties as a result of Defendants' actions; BNY has wrongfully prevented Hammond from taking prompt measures to protect himself through BNY's unreasonable delay in notifying Hammond; and the remedies being offered by BNY are insufficient to make Hammond whole or otherwise adequately protect him from identity theft, all of which has caused him to suffer from distress and disturbance to his peace of mind.

8. Plaintiff Linda Young ("Young") is a resident of Ellwood City, Pennsylvania. On or around June 9, 2008, Young received a letter from Defendant BNY notifying her that an unencrypted back-up tape that "may" include Young's Sensitive Personal Information was "lost" while being transported from BNY's processing site in Philadelphia to its data storage site in Pittsburgh. As a result of Defendants' conduct alleged herein, Young has suffered injuries. Specifically, Young's private, nonpublic personal and financial information has been improperly and illegally compromised and/or disseminated to third parties as a result of Defendants' actions; BNY has wrongfully prevented Young from taking prompt measures to protect herself through BNY's unreasonable delay in notifying Young; and the remedies being offered by BNY are insufficient to make Young whole or otherwise adequately protect her from identity theft, all of which has caused her to suffer from distress and disturbance to her peace of mind.

9. Plaintiff William H. Wicks ("Wicks") is a resident of Manilus, New York. Wicks was notified by BNY Mellon Shareowner Services that his Sensitive Personal Information was contained on one of the missing tapes. As a result of Defendants' conduct alleged herein, Wicks has suffered injuries. Specifically, Wicks' private, nonpublic personal and financial information has been improperly and illegally compromised and/or disseminated to third parties as a result of Defendants' actions; BNY has wrongfully prevented Wicks from taking prompt measures to protect himself through BNY's unreasonable delay in notifying Wicks; and the remedies being offered by BNY are insufficient to make Wicks whole or otherwise adequately protect him from identity theft, all of which has caused him to suffer from distress and disturbance to his peace of mind.

10. Defendant BNY is a Delaware corporation with a principal place of business located at One Wall Street, New York, New York 10286. BNY describes itself as "a global

financial services company focused on helping clients manage and service their financial assets, operating in 34 countries and serving more than 100 markets. The company is a leading provider of financial services for institutions, corporations and high-net-worth individuals, providing superior asset management and wealth management, asset servicing, issuer services, clearing services and treasury services through a worldwide client-focused team.” According to its most recent Form 10-K filed with the Securities and Exchange Commission, Defendant BNY was created on July 1, 2007 following a merger of The Bank of New York Company, Inc. and Mellon Financial Corporation. BNY has approximately \$1.121 trillion in assets under management, and \$23.1 trillion in assets under custody and administration. Securities of BNY are publicly traded on the New York Stock Exchange under the ticker “BK.” BNY and its subsidiaries have over 42,000 employees.

11. Defendant BNY’s website, <http://www.bnymellon.com>, touts the importance BNY attributes to protecting the privacy of personal information with which it is entrusted, with a reference to its “internal policies governing use and disclosure of such confidential information” to reassure the public about its ability to maintain the security of confidential information.

12. Various other individual persons and entities (including, without limitation, companies with which BNY contracts and accordingly permits to transport the Sensitive Personal Information of Plaintiffs and Class members), the identities of whom are presently unknown to Plaintiffs and their counsel, have performed acts in furtherance of the conduct complained of herein, and/or are otherwise jointly and severally liable with BNY. Collectively, these defendants shall be referred to herein as the “John Doe Defendants.” The acts charged in

this Complaint have been done by BNY and the John Doe Defendants, and/or were authorized, ordered or done by their respective officers, agents, employees or representatives.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds \$5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A).

14. This Court has personal jurisdiction over Defendants because they own and operate a business that is located within this state, and conduct substantial business throughout the United States.

15. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the acts giving rise to Plaintiffs' claims occurred in this district, and because Defendant BNY is headquartered and conducts substantial business in this judicial district.

FACTUAL BACKGROUND

16. In connection with the functions that it performs on behalf of its institutional and corporate clients, Defendant BNY is provided and entrusted with the confidential Sensitive Personal Information of millions of people. Many of BNY's clients contract with BNY to administer services concerning shareholders. By way of example, it has been reported that People's United Bank ("People's United") provided BNY with the Sensitive Personal Information of its shareholders/depositors as part of the process of converting People's United into a public company. People's United was reportedly required to provide all of its shareholders/depositors with the opportunity to vote on the conversion, and BNY was

accordingly provided with their Sensitive Personal Information so that it could disseminate and tabulate their votes.

A. The February 2008 Security Breach.

17. The first BNY security breach occurred in February of 2008. On February 27, 2008 an archive service vendor selected by BNY to transfer the confidential Sensitive Personal Information of Plaintiffs and Class members informed BNY that it “could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility.” The data backup tapes that were in the missing box contained, among other things, the Social Security numbers of consumers. Upon information and belief, this data intrusion occurred in New Jersey, and involved data from BNY’s Shareholder Services unit.

18. Inexplicably, BNY unreasonably delayed notifying consumers, the primary owners of the Sensitive Personal Information, of the February 2008 incident. In the May 21, 2008 letter to BNY, Attorney General Blumenthal writes that “I am especially concerned by the delay in informing consumers, possibly heightening the risks of wrongdoing. Neither [People’s United], nor its customers were promptly notified. Even now, many may be in the dark.”

19. It has been reported that BNY took more than eight (8) weeks to notify the affected institutions of the breach from the February 2008 incident. Even more astounding, it has been reported that many consumers who were potentially impacted by this incident that took place months ago *still have not received letters from BNY* notifying them of the breach and cautioning them that their Sensitive Personal Information may have been compromised. Needless to say, it is critical for these consumers to be promptly notified that their Sensitive Personal Information has been (or may have been) jeopardized so that they can take appropriate

steps to protect their identity, such as immediately implementing a credit freeze and/or closely monitoring their credit reports.

20. Upon information and belief, many consumers that have attempted to contact BNY have been unable to get a straight answer as to whether their Sensitive Personal Information was actually compromised by the data intrusion.

21. In the aftermath of the February 2008 incident, BNY initially offered consumers 12 months worth of free credit monitoring. According to one of the letters that was sent out by BNY after the breach, consumers were given 90 days from the date of the letter to enroll in the free credit monitoring program offered by BNY.

22. On May 30, 2008 Attorney General Blumenthal's office – in connection with the Connecticut Department of Consumer Protection – issued a press release that set forth the “top 25 companies with the most Connecticut residents affected by the Bank of New York Mellon data breach.” These companies are listed below, with the approximate number of affected Connecticut residents in parenthesis:

- People's United Financial Inc. (403,894)
- John Hancock Financial Services, Inc. (*acquired by Manulife Financial Corporation*) (33,586)
- The Walt Disney Company (18,361)
- TD Bank Financial Group (9,389)
- The Bank of New York Mellon Corporation (3,324)
- Hudson United Bancorp (*acquired by TD Bank Financial Group*) (2,703)
- United Parcel Service, Inc. (2,075)
- Wachovia Corporation (1,479)
- MetLife, Inc. (1,373)

- Hudson City Bancorp (601)
- Eastman Kodak Company (456)
- Burlington Resources (*acquired by ConocoPhillips Inc.*) (447)
- Provident Financial (*acquired by Washington Mutual, Inc.*) (404)
- Penn Fed Financial (*acquired by New York Community Bancorp*) (360)
- ADESA, Inc. (277)
- Alcatel-Lucent (243)
- Odyssey America Reinsurance Corporation (232)
- Seacoast Financials Services Corp. (*acquired by Sovereign Bancorp*) (216)
- Viewpoint Bank (213)
- Diamond Shamrock (*acquired by ConocoPhillips Inc.*) (211)
- Sound Federal Bancorp (*acquired by Hudson City Bancorp*) (199)
- Big Lots, Inc. (192)
- Guidant Corporation (*acquired by Boston Scientific Corp*) (126)
- New York Community Bancorp (126)
- ACE Ltd. (119)

23. In all, the February 2008 incident reportedly involved the Sensitive Personal Information from consumers, investors, and/or employees of more than seven hundred (700) companies and institutions. The Sensitive Personal Information of some 4.5 million consumers nationwide was compromised by the February 2008 incident. Through no fault of their own, these individuals are now all at a substantially increased risk of identity theft and fraud.

B. The April 2008 Security Breach.

24. The confidential Sensitive Personal Information of consumers that was entrusted to BNY was subject to yet another data intrusion on or around April 29, 2008. On this occasion, an unencrypted back-up tape that “may” contain consumers’ Sensitive Personal Information was “lost while being transported by an outside carrier from [BNY’s] processing site in Philadelphia, PA to its data storage site in Pittsburgh, PA.”

25. The April 2008 incident reportedly involved data from forty-seven (47) of BNY’s institutional clients, and a yet to be determined number of individual consumers. Upon information and belief, the April 2008 incident involved a different business unit of BNY: the BNY Mellon Working Capital Solutions unit. This unit is reportedly responsible for processing payments on behalf of BNY’s institutional clients, such as pension funds and mutual funds.

26. Yet again, BNY delayed notifying consumers, the primary owners of the Sensitive Personal Information, of the breach. It has been reported that BNY did not complete notifying the forty-seven (47) institutional clients that were affected by this breach until May 16, 2008. Plaintiff Young’s Sensitive Personal Information was at risk of being compromised as a result of the April incident this whole time, yet she did not receive a letter from BNY informing her that her Sensitive Personal Information may have been compromised until June 7, 2008 – nearly 6 weeks after the breach had occurred, and several weeks after BNY had already finished first notifying its corporate clients.

27. The June 7, 2008 letter to Plaintiff Young indicates that BNY is implementing certain unspecified “additional security procedures” to help ensure that there is not another data intrusion. In addition, BNY offers Young and the recipients of this ostensible form letter an

opportunity to receive “credit report monitoring services for two years, at no cost,” and identity theft insurance (where not prohibited by state law) up to \$25,000.

C. Federal Legislation and Regulations.

28. The GLB requires companies defined under the law as “financial institutions” to ensure the security and confidentiality of personal information entrusted to them, including names, addresses, and phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers. The GLB sets forth the minimum privacy protections mandated by financial services companies.

29. Defendant BNY is a “financial institution” within the definition of GLB and implementing regulations.

30. Pursuant to § 505 of the GLB, four of the eight federal agencies charged with its implementation promulgated regulations implementing the privacy and security provisions of the GLB: 12 C.F.R. Part 30, App. B contains regulations of the Office of the Comptroller of the Currency, Treasury (“OCC”); 12 C.F.R. Part 208, App. D-2 and Part 225, App. 5 contain regulations of the Board of Governors of the Federal Reserve System (“Board”); 12 C.F.R. Part 364, App. B contains regulations of the Federal Deposit Insurance Corporation (“FDIC”) and 12 C.F.R. Part 570, App. B contains regulations of the Office of Thrift Supervision, Treasury (“OTS”).

31. Following an extensive notice and comment period, the four agencies (OCC, Board, FDIC and OTS) issued Interagency Guidelines Establishing Information Security Standards (the “Security Guidelines”) that sets forth minimum mandatory measures, including response programs and customer notification procedures that a financial institution *must* develop and implement in the event of an unauthorized access to or use of customer information.

32. The Security Guidelines require a financial institution to, *inter alia*, assess and address the following risks:

- reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- the likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and
- the insufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

33. The Security Guidelines direct every financial institution to “enter into a contractual commitment with its Service Providers to implement appropriate measures designed to protect against unauthorized access to or use of customer information.”

34. The Security Guidelines give financial institutions “an affirmative duty” to protect their customers’ information against unauthorized access or use. Notification of customers of a security incident involving the unauthorized access is a key part of that duty.

35. At a minimum, the notification must be timely, given in a clear and conspicuous manner, describe what the institution has done to protect the customers’ information from further unauthorized access, and include a working telephone number that is staffed with trained personnel to respond to customer inquiries and requests for assistance.

36. The four agencies, OCC, Board, FDIC and OTS, specifically rejected the request made in the notice and comment period that compliance with the Security Guidelines creates a “safe harbor” defense from class action lawsuits citing to § 507 of GLB that specifically states the Act does not exempt state laws that offer greater consumer protection than the GLB.

37. In addition to the Security Guidelines, the Federal Trade Commission (“FTC”), another agency charged with implementing the privacy policies of the GLB, issued its “Safeguards Rule” which apply to financial institutions and other institutions handling confidential customer information. 16 C.F.R. Part 314, 67 Fed. Reg. 36493 (May 23, 2002).

38. The Safeguards Rule requires financial institutions, including Defendant BNY, to develop a written information security plan that describes their program to protect customer information. The Safeguards Rule states that the security plan must, at a minimum:

- a. take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
- b. require service providers by contract to implement and maintain such safeguards; and
- c. evaluate and adjust the information security program in light of the results of the testing and monitoring required by the regulations, and material changes to the business operations, or any other circumstances that you know or have reason to know may have a material impact on the information security program.

D. New York State Business Law.

39. Pursuant to New York General Business Law § 899-aa any person which conducts business in N.Y. state . . . must [following a security breach that compromises] private information (defined as “social security number, . . . or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account”) disclose the breach to the affected person “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.” § 899-aa.2 of New York General Business Law.

40. In the event of a failure to adhere to this provision a court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. In addition where the violation was knowing or reckless the court may impose a civil

penalty of the greater of \$5,000 or up to \$10 per instance of failed notification, provided that the later amount not exceed \$150,000.

E. Defendant BNY's Inadequate Remedial Scheme.

41. Defendant BNY is now offering eligible consumers two years worth of free credit monitoring, \$25,000 worth of identity theft insurance “where permitted by local law,” and free “credit freezes.”¹ BNY has also set up a toll free hotline that is open six days a week that consumers can call with inquiries. These measures are wholly inadequate and insufficient to appropriately compensate and protect Plaintiffs and Class members from the substantially increased risk of identity theft, and are completely without any mechanism to compensate and assist persons once the identity theft occurs.

42. In the May 30, 2008 press release, Attorney General Blumenthal indicated that there had been no reports of actual identity theft, but acknowledged that “the risk [of identity theft] may last for months or years.”

43. The steps taken by BNY to compensate and protect consumers for its negligent misconduct are woefully inadequate, and are disproportionately small in comparison to data breaches in similar situations. For example, a series of data breaches that occurred at various points between 2002 and 2006 at TJX – which operates thousands of retail stores across the United States – compromised certain personal and financial information of millions of consumers, including credit and debit card information, drivers’ licenses, military, and state identification numbers (which sometimes were identical to consumers’ Social Security numbers),

¹ A “credit freeze” is a service provided by credit rating agencies – for a fee – whereby a consumer’s credit is “frozen,” making it impossible for anyone, including the consumer, to take out a new line of credit or to open up a new credit card account. If the consumer wishes to obtain new credit, he or she typically pays another fee to “unfreeze” their credit information.

and check transaction information. Significantly – and unlike the current case – it appears that the data breach at TJX only included consumers’ Social Security numbers to the extent that they were the same as the numbers that appeared on those consumers’ state drivers licenses or other forms of identification that were compromised. Nevertheless, TJX has preliminarily² offered to settle a series of consumer class action lawsuits that were filed against it in connection with this data breach for, among other things, *three years* worth of free credit monitoring for consumers whose Sensitive Personal Information may have been compromised, cash reimbursement for certain out-of-pocket expenditures associated with the data breach, vouchers or cash alternatives, and a dispute resolution program for any claims related to possible identity theft.

44. The instant case is even more egregious than the breach at issue in the TJX case because, *inter alia*, the intrusion at BNY included the Social Security numbers of many – if not all – of the affected consumers. Unlike a data breach involving the theft of a consumers’ credit or debit card account information, which can simply be canceled, the theft of a consumer’s Social Security number and other Sensitive Personal Information puts that consumer at risk of identity theft for the rest of his or her life – and possibly even beyond.

45. In light of the severe nature of the breach at issue in this case – and based on the steps that have been taken by other companies like TJX to remedy less serious invasions in other cases – the reasonable standards in the industry require BNY to do much more to protect the privacy interests of the millions of affected consumers that have been injured and that are at a substantially increased risk of identity fraud as a result of BNY’s misconduct.

² The preliminary settlement in this case, *In Re: TJX Companies Retail Security Breach Litigation*, which is pending before the Honorable William G. Young in the United States District Court for the District of Massachusetts, is subject to final approval by the court.

46. This case is brought to ensure that the consumers affected by the massive data breach at BNY are appropriately compensated, and are adequately protected from the future misuse of their Sensitive Personal Information. These are not trivial or inconsequential concerns. Indeed, Attorney General Blumenthal's May 21 letter to BNY describes the breach from the February incidents as "highly dangerous, indeed possibly devastating," and expresses concerns with "the possibility that credit card fraud and identity loss may result from the breach of this sensitive and personally identifying information."

47. In addition to offering consumers an unreasonably abridged period of free credit monitoring, BNY is not offering identity theft insurance to consumers in states (such as New York) where such insurance coverage is prohibited by applicable laws. The extent to which BNY will indemnify or protect consumers who live in such states – if at all – from identity theft as a result of its negligence, is unclear. Further, there is no alternative dispute resolution or other program being offered by BNY whereby consumers who may have suffered actual identity fraud as a result of BNY's negligence may submit claims or grievances to BNY to be reimbursed for their out-of-pocket expenses.

48. In its June 7, 2008 letter, BNY also encourages consumers to place a credit or security freeze on their credit files. However, as the letter points out, "using a credit or security freeze may delay your ability to obtain credit." BNY offers to cover the cost of the "initial placement and one removal (whether a temporary or permanent removal) of a credit or security freeze even if [the consumer] is not the victim of identity theft," so long as the recipient does so within 90 days of receipt of the letter. This letter goes on to advise, however, that "[b]ecause credit or security freezes can be temporarily removed on more than one occasion, you may incur

costs associated with having a credit or security freeze on your credit file *that BNY Mellon will not cover.*" (emphasis supplied).

CLASS ACTION ALLEGATIONS

49. This action is brought on behalf of Plaintiffs, individually and as a class action, pursuant to FED. R. CIV. P. 23(a), (b)(2) and (b)(3) on behalf of all consumers whose Sensitive Personal Information was provided to BNY, and which was accessed and/or compromised. The Class does not include Defendants, or their officers, directors, agents, or employees, or any attorneys that represent the Plaintiffs in this action.

50. Specifically, Plaintiffs seek to represent the following Classes:

Nationwide Class: All persons in the United States whose Sensitive Personal Information was provided to BNY, and which was accessed and/or compromised from either or both security breaches.

New York Sub-Class: All persons in New York whose Sensitive Personal Information was provided to BNY, and which was accessed and/or compromised from either or both security breaches.

Michigan Sub-Class: All persons residing in Michigan whose Sensitive Personal Information was provided to BNY, and which was accessed and/or compromised from either or both security breaches.

Pennsylvania Sub-Class: All persons residing in Pennsylvania whose Sensitive Personal Information was provided to BNY, and which was accessed and/or compromised from either or both security breaches.

51. The Nationwide Class is comprised of literally millions of consumers, the joinder of whom in one action is impracticable. The Michigan, Pennsylvania and New York Sub-Classes are likewise sufficiently large to make joinder impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

52. The rights of each member of the Class were violated in a similar fashion based upon Defendants' uniform actions.

53. Questions of law and fact common to the Class predominate over questions which may affect individual Class members, and include the following:

- a. whether Defendants were negligent in collecting and storing the Sensitive Personal Information of Plaintiffs and Class members;
- b. whether Defendants took reasonable measures to safeguard the Sensitive Personal Information of Plaintiffs and Class members;
- c. whether Defendants owed a duty to Plaintiffs and/or the Class to protect the Sensitive Personal Information of Plaintiffs and Class members;
- d. whether Defendants breached this duty to exercise reasonable care in storing the Sensitive Personal Information of Plaintiffs and Class members by, *inter alia*, failing to select a competent courier, or service provider, to transport the Sensitive Personal Information of Plaintiffs and Class members, storing the Sensitive Personal Information of Plaintiffs and Class members in an unencrypted format, and by failing to adequately supervise and monitor its couriers;
- e. whether Defendants breached a duty by failing to keep Plaintiffs and Class members' personal and financial information secure; whether Defendants' conduct violates the Michigan, New York and Pennsylvania Consumer Protection statutes;
- f. whether Plaintiffs and members of the Class are entitled to compensation, monetary damages, and/or additional services/corrective measures from BNY and, if so, the nature and amount of any such relief; and
- g. whether statutory and trebled damages are proper in this matter.

54. Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no interest that is antagonistic to or that irreconcilably conflicts with the interests of other members of any of the Classes.

55. Plaintiffs have retained counsel competent and experienced in the prosecution of class action litigation.

56. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiffs' and the Class members' claims. Plaintiffs and the members of each Class have suffered immediate irreparable harm as a result of Defendants' deceptive, negligent, and unlawful conduct. The damages suffered by individual Class members may be relatively small, and thus few, if any individual Class members can afford to seek legal redress on an individual basis for the wrong complained of herein. Absent a class action, Plaintiffs and members of each of the Classes will continue to suffer losses as a result of Defendants' unlawful and negligent conduct, and will not be adequately protected and compensated therefore.

57. Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the Classes, thereby making appropriate equitable relief with respect to Plaintiffs and the Classes as a whole.

**COUNT I - VIOLATION OF THE MICHIGAN
CONSUMER PROTECTION ACT**
(Against All Defendants)

58. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Michigan Sub-Class**.

59. Plaintiffs entrusted their Sensitive Personal Information to Defendants primarily for their personal, family and household purposes.

60. Defendants' conduct alleged herein violates the Michigan Consumer Protection Act, MCL 445.901, *et. seq.*, including, but not necessarily limited to the following sections thereof:

- a) § 445.903(s), by failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer.
- b) § 445.903(bb), by making a representation of fact or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is.
- c) § 445.903(cc), by failing to reveal facts which are material to the transaction in light of representations of fact made in a positive manner.

61. Neither Plaintiffs, nor any other Class member, would have entrusted or consented to provide their Sensitive Personal Information to BNY and the John Doe Defendants had they known, *inter alia*, that BNY would not ensure that adequate measures were taken to protect this highly sensitive confidential information, and that, in the event of a security breach, BNY would not give timely notice, or take appropriate and meaningful measures to adequately compensate and protect consumers.

62. As a result of Defendants' violation of the Michigan Consumer Protection Act, Plaintiffs and members of the Class have incurred damages.

63. Plaintiffs demand actual, statutory, and treble damages.

**COUNT II - VIOLATION OF THE PENNSYLVANIA
UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW**
(Against All Defendants)

64. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Pennsylvania Sub-Class**.

65. The conduct alleged above constitutes unfair methods of competition or unfair or deceptive acts or practices in violation of Section 201-2(4)(v),(vii), (xiv) and (xxi) of the Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 Pa.C.S.A. §§ 201-1, *et seq.*

66. The UTPCPL applies to the claims of Plaintiff Young and the other members of the Pennsylvania Sub-Class because the conduct which constitutes violations of the UTPCPL by the Defendants occurred in substantial part within the Commonwealth of Pennsylvania.

67. Plaintiff Young and the other members of the Pennsylvania Sub-Class are consumers who provided their Sensitive Personal Information to BNY and its agents, and did so primarily for personal, family or household purposes within the meaning of 73 Pa.C.S.A. § 201-9.2.

68. Defendants used and employed unfair methods of competition and/or unfair or deceptive acts or practices within the meaning of 73 Pa.C.S.A. §§ 201-2 and 201-3.

69. Defendants' concealments, omissions, deceptions and conduct were likely to deceive and likely to cause misunderstanding and/or in fact caused Plaintiff Young and the other members of the Pennsylvania Sub-Class to be deceived.

70. Defendants intended that Plaintiff Young and the other members of the Pennsylvania Sub-Class would rely on its misrepresentations, concealment, warranties, deceptions and/or omissions.

71. Plaintiff Young and the other members of the Pennsylvania Sub-Class have been damaged as a proximate result of BNY's violations of the UTPCPL and have suffered actual, ascertainable losses.

72. As a direct and proximate result of BNY's violations of the UTPCPL as set forth above, Plaintiff Young and the other members of the Pennsylvania Sub-Class have suffered an ascertainable loss of money and are therefore entitled to relief, including damages, plus triple damages, costs and attorney's fees under Section 201-9.2 of the UTPCPL.

**COUNT III - VIOLATION OF SECTION 349 OF THE
NEW YORK GENERAL BUSINESS LAW
(Against All Defendants)**

73. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **New York Sub-Class**.

74. Plaintiff Wicks is a consumer who resides in New York.

75. Defendants have engaged in unfair and deceptive practices, as described herein, in violation of §349 of the New York General Business Law.

76. These unfair and deceptive practices have directly and proximately caused injury to Wicks and other members of the New York Sub-Class. Plaintiffs and the other members of the New York Sub-Class seek damages and treble damages as permitted by § 349 of the New York General Business Law.

COUNT IV – NEGLIGENCE
(Against All Defendants)

77. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

78. Defendants, upon coming into possession of Plaintiffs and the Class' private, non-public, personal and financial information, had a duty to exercise reasonable care in safeguarding

and protecting such information from being compromised and/or stolen. This duty arises from the common law, as well as from those duties expressly imposed upon Defendants from sources such as contracts between Plaintiffs and Class members and third parties, agreements between Defendants and third parties, and industry standards.

79. Defendants also had a duty to timely disclose the fact that Plaintiffs and the Class' private, non-public personal and financial information within their possession had been, or was reasonably believed to have been, compromised.

80. Defendants also had a duty to have procedures in place to detect and prevent dissemination of Plaintiffs' private information to third parties. This breach of security and unauthorized access was reasonably foreseeable to BNY.

81. Defendants, through their acts and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and the Class' private, non-public Sensitive Personal Information within their possession.

82. Defendants, through their actions and/or omissions, breached their duty to Plaintiffs and the Class by failing to have adequate procedures in place to detect and prevent dissemination of Plaintiffs' private information to third parties. Defendants also breached this duty by storing (or causing to be stored) the Sensitive Personal Information of Plaintiffs and Class members in an unencrypted, readily accessible format.

83. Defendants, through their actions and/or omissions, breached their duty to timely disclose the fact that Plaintiffs and the Class' private, non-public personal and financial information within its possession had been, or was reasonably believed to have been, compromised.

84. But for BNY's negligent and wrongful breach of its duties owed to Plaintiffs and the Class, Plaintiffs' and the Class' private non-public personal and financial information would not have been compromised.

85. Plaintiffs and Class members' private, non-public, personal and financial information was compromised, viewed, and/or stolen as the proximate result of BNY failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures to protect and safeguard the private, non-public, personal and financial information within its possession.

86. Plaintiffs and the Class have and/or can be expected to incur actual damages, including, but not limited to: expenses to prevent identity theft, credit monitoring for an adequate period of time, anxiety, emotional distress, loss of privacy, loss of peace of mind, the increased exposure to identity theft, and other economic and non-economic harm.

**COUNT V - BREACH OF CONTRACTS TO WHICH PLAINTIFFS
AND CLASS MEMBERS WERE THIRD-PARTY BENEFICIARIES**
(Against All Defendants)

87. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

88. Upon information and belief, Plaintiffs and Class members are third-party beneficiaries of contracts entered into between Defendants and third parties, such as the employers and/or banks and/or corporations with which Plaintiffs and Class members are employed, or transact financial business or hold investments, or transact any other business. These third parties include, without limitation, the entities listed above in ¶ 22.

89. Plaintiffs and Class members are also third-party beneficiaries of contracts between BNY and the couriers that BNY hires to protect and transport their Sensitive Personal Information.

90. Upon information and belief, these contracts between BNY and third parties require, *inter alia*, that Defendants safeguard the Sensitive Personal Information of Plaintiffs and the Class.

91. Defendants breached these agreements, causing injury to Plaintiffs and the Class.

COUNT VI - BREACH OF IMPLIED CONTRACT
(Against All Defendants)

92. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

93. Coming into possession of Plaintiffs' and the Class' private, non-public, personal and financial information also created an implied contract with Plaintiffs and the Class to protect such information.

94. The implied contract required Defendants to not disclose the Plaintiffs' or Class' private, nonpublic Sensitive Personal Information and to safeguard and protect the information from being compromised and/or stolen.

95. Defendants did not safeguard and protect Plaintiffs and the Class' private, nonpublic, personal and financial information from being compromised and/or stolen. To the contrary, Defendants allowed this information to be disclosed to an unauthorized third party.

96. Because Defendants disclosed Plaintiffs' and Class members' private, non-public Sensitive Personal Information and failed to safeguard and protect Plaintiffs and the Class' private, nonpublic, personal and financial information from being compromised and/or stolen, BNY breached its contract with Plaintiffs and the Class.

97. Plaintiffs and the Class have and/or can be expected to incur actual damages, including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

COUNT V – NEGLIGENCE *PER SE*
(Against All Defendants)

98. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

99. The Defendants violated numerous provisions of the regulations implemented to effectuate the GLB, including:

- a. failure to adequately assess or address the risk of transporting unencrypted tapes, taking into account the sensitivity of customer information;
- b. failure to maintain policies, procedures, customer information systems, and other arrangements to control risks;
- c. failure to implement appropriate measures with its service providers to protect against unauthorized access;
- d. failure to notify customers in a timely manner;
- e. failure to describe in the notice what it did to protect the customers' information from further unauthorized access; and
- f. failure to evaluate and adjust its program as the results of security breaches.

100. The regulations promulgated by the federal agencies charged with implementing GLB, the ("Security Guidelines" issued by OCC, the Board, FDIC and OTS) and the ("Safeguards Rule" issued by the FTC) establish the minimal duty of care owed by the Defendants to the named Plaintiffs and Plaintiff Class.

101. Defendants failed to meet that minimal duty.

102. Named Plaintiffs and Plaintiff Class are entitled to rely on Defendants' liability *per se* in that Defendants' failure to adhere to regulatory requirements constitutes as a matter of law negligence *per se*.

103. Defendants' negligence *per se* is a proximate cause of the injuries inuring to Plaintiffs and the Class.

COUNT VI – GROSS NEGLIGENCE
(Against All Defendants)

104. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

105. After BNY knew of the risk of a security breach caused by transporting unencrypted sensitive personal data entrusted to it, as a result of the February 2008 security breach, nevertheless in the face of that known risk, BNY failed to change its security protection practices and thereby through its gross negligence, it permitted the April 2008 security breach to occur.

106. But for BNY's negligent and wrongful breach of its duties owed to Plaintiffs and the Class, Plaintiffs' and the Class' private non-public personal and financial information would not have been compromised.

107. Plaintiffs and Class members' private, non-public, personal and financial information was compromised, viewed, and/or stolen as the proximate result of BNY failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures to protect and safeguard the private, non-public, personal and financial information within its possession.

108. Plaintiffs and the Class have and/or can be expected to incur actual damages, including, but not limited to: expenses to prevent identity theft, credit monitoring for an adequate period of time, anxiety, emotional distress, loss of privacy, loss of peace of mind, the increased exposure to identity theft, and other economic and non-economic harm.

**COUNT VII – VIOLATION OF SECTION 899-aa OF THE
NEW YORK GENERAL BUSINESS LAW
(Against All Defendants)**

109. Plaintiffs incorporate the allegations in the preceding paragraphs. This Count is brought on behalf of the **Nationwide Class**.

110. The Defendants violated § 899-aa of the New York General Business Law that applies to “any person or business which conducts business in New York State” by *inter alia* failing to give notice “in the most expedient time possible and without unreasonable delay” to the affected Class members.

111. Plaintiffs and Class members are among the class of people for whose particular benefit this statute has been enacted. A private right of action under this statute would promote the legislative purpose behind the statute, and creation of a private right would be consistent with and in furtherance of the overall legislative scheme.

112. BNY’s violation of § 899-aa of the New York State General Business Law was done knowingly and recklessly since it knew about its obligations to give notice as expeditiously as possible as a result of the February 2008 breach, and yet knowingly and with contempt for the provisions of New York State law continued to fail to give expeditious notice to victims of the April 2008 security breach.

113. Plaintiffs and Plaintiff Class seek consequential financial damages and a civil penalty up to the maximum allowed by § 899-aa.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that this Court enter an Order:

(a) certifying this matter as a class action, appointing Plaintiffs as Class representatives and designating Plaintiffs' counsel as class counsel;

(b) granting an award against Defendants for actual, statutory, punitive, treble and/or compensatory damages, as provided by the Pennsylvania, New York, and Michigan Consumer Protection Acts, and the common law and contractual claims asserted herein;

(c) granting an award against Defendants for actual, statutory, punitive, treble and/or compensatory damages, as provided by the Pennsylvania, New York, and Michigan Consumer Protection Acts, and enjoining Defendants from continuing their unfair and/or deceptive conduct;

(d) finding that Defendants were negligent in protecting Plaintiffs' and the Class' Sensitive Personal Information, and based on their failure to take appropriate measures after they first became aware of each breach, and finding that this conduct caused foreseeable injuries to Plaintiffs and Class members;

(e) finding the Defendants were negligent *per se* by violating various regulations issued under the GLB Act and finding that this conduct was the proximate cause of foreseeable injury to Plaintiffs and Class members;

(f) finding the Defendants were grossly negligent and finding that their conduct was the proximate cause of foreseeable injury to Plaintiffs and Class members;

(g) finding the Defendants violated the provisions of § 899-aa of the New York General Business Law and such a violation was knowing and reckless entitling Plaintiffs

and Plaintiff Class to pursue a private right of action and to receive consequential financial damages and civil penalties to the full extent of the law;

(h) finding that Defendants breached their duty to safeguard and protect Plaintiffs' and the Class' Sensitive Personal Information;

(i) awarding damages to Plaintiffs and the Class, as well as reasonable attorneys' fees and costs of litigation;

(j) awarding injunctive relief against the Defendants designed to prevent the loss of Sensitive Personal Information by BNY in the future, and requiring Defendants to offer a full and fair compensation plan to Plaintiffs and Class members who have already suffered from the February 2008 and April 2008 security breaches; and

(k) providing for such other legal and/or equitable relief as justice requires.

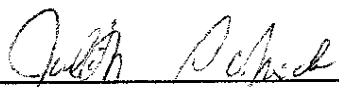
JURY DEMAND

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Dated: July 1, 2008

Respectfully submitted,

By:


Judith Scolnick (JS0827)
SCOTT + SCOTT LLP
29 West 57th Street
New York, NY 10019
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
E-Mail: jscolnick@scott-scott.com

CHIMICLES & TIKELLIS LLP
Joseph G. Sauder (PA ID 82467)
Matthew D. Schelkopf (PA ID 89143)
Benjamin F. Johns (PA ID 201373)

One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
E-mail: JosephSauder@chimicles.com
matthewschelkopf@chimicles.com
BFJ@chimicles.com

Christopher G. Hayes (PA ID No. 57253)
LAW OFFICE OF
CHRISTOPHER G. HAYES
225 South Church Street
West Chester, PA 19382
Telephone: (610)-431-9505
Facsimile: (610)-431-1269
E-mail: chris@chayeslaw.com

**ATTORNEYS FOR PLAINTIFFS AND THE
PROPOSED CLASS**

EXHIBIT A

State of Connecticut

RICHARD BLUMENTHAL
ATTORNEY GENERAL



Hartford
May 21, 2008

VIA ELECTRONIC MAIL AND FIRST CLASS U.S. MAIL

Stephen Dalmatch
General Counsel
Bank of New York Mellon Shareowner Services
480 Washington Avenue
Jersey City, NJ 07310

RE: The Bank of New York Mellon Security Breach -- Missing Back-up Tapes

Dear Mr. Dalmatch:

I am alarmed and deeply concerned by a recent and serious data breach at The Bank of New York Mellon ("BNY") involving the loss of computer back-up tapes containing sensitive information of some 4.5 million consumers, including People's United Bank account holders and shareowners. Several hundred thousand Connecticut citizens may be affected, and possibly more, by this loss of highly significant personal information.

BNY representatives informed my office that the information on the tapes contained, at a minimum, Social Security numbers, names and addresses, and possibly bank account numbers and balances. I am especially concerned about the possibility that credit card fraud and identity loss may result from the breach of this sensitive and personally identifying information.

According to the information you provided, a metal box with six to ten unencrypted back-up bank tapes containing confidential personal information was "lost" in February, 2008 from a truck owned by Archival Systems, Inc., a company that transports and "securely" stores these types of tapes in its storage facility. The lock on the truck was broken -- possibly before the beginning of the workday -- and the truck was left unattended several times. Ten boxes from BNY were placed on the truck. Only nine reached the storage facility.

This security breach seems highly dangerous, indeed possibly devastating in light of the identity theft threat. You have also informed this office that BNY began notifying the affected customers six weeks ago and is offering one year of credit monitoring through Equifax. Given this extraordinarily serious security breach, this offer of protection is grossly inadequate. Connecticut agencies that have experienced data security breaches less serious in magnitude or

potential damage have offered consumers two years of credit monitoring, \$25,000 identity theft insurance and free credit freezes BNY should do no less

Given the possible devastating impact on consumers in Connecticut, my office requests more detailed information -- in full and in writing -- on how this breach occurred, what steps have been taken to protect these individuals, and what new procedures have been adopted to prevent future data breaches.

For the purposes of this letter and the questions below, "You" and "Your" refer to BNY. Please provide responses to the following by May 30, 2008:

- 1 Prior to the loss of this data, what measures did You take to safeguard sensitive information of the sort contained on the lost back-up tapes;
- 2 Please indicate how and when You first learned of the loss of the back-up tapes;
- 3 Please describe in detail the circumstances under which the back-up tapes were lost;
4. Please identify the total number of Connecticut consumers that may possibly be affected by the loss of the back-up tapes;
- 5 Please identify each issuer (client of Yours) which had its clients/shareholders/customers' information on one of the missing back-up tapes and, for each, identify the number of Connecticut residents that may possibly be affected by the loss of the back-up tapes;
6. Please describe in detail the categories of consumer information compromised by the loss including, but not limited to, name, address, Social Security Number, or other sensitive information;
- 7 Please describe all steps that You have taken to track down and retrieve the missing back-up tapes and the sensitive files and information contained thereon;
- 8 Please describe all steps You have taken or will take to contact and warn consumers that their sensitive and personally identifying information may have been compromised including, but not limited to, when and how You first notified consumers of this loss, and whether You will individually notify each consumer about the loss;
- 9 Please identify all steps You have taken or will take to protect those consumers whose personal information may have been or was actually compromised from

identity theft and credit card fraud, including, but not limited to, any credit monitoring or identity restoration services and insurance that has been or will be offered to these consumers;

10. Please provide an outline of the plan You have developed to prevent the reoccurrence of such a loss and a timeline for implementing that plan;
11. Please describe Your general corporate policies regarding securing back-up tapes such as the lost tapes that are the subject of this letter, and the personally identifying information contained thereon; and
12. Please identify each instance where a back-up tape was lost in the past and, for each incident, state whether such tape contained any sensitive, personally identifiable information

I am especially concerned by the delay in informing consumers, possibly heightening the risks of wrongdoing. Neither People's nor its customers were promptly notified. Even now, many may be in the dark.

The loss of these tapes -- so far unrecovered and unremedied -- is inexplicable and unacceptable. It must be addressed by protective measures to forestall identity theft immediately

I appreciate your cooperation in this matter and look forward to hearing from you. The information requested herein should be sent to Assistant Attorneys General Matthew Fitzsimmons and Phillip Rosario at 110 Sherman Street, Hartford, Connecticut 06105. Should you have any questions, you may contact Assistant Attorneys General Fitzsimmons or Rosario at (860) 808-5400. Thank you

Very truly yours,



RICHARD BLUMENTHAL

RB/pas

EXHIBIT B



THE BANK OF NEW YORK MELLON

June 7, 2008

Dear MetLife Customer:

The Bank of New York Mellon processes payments on behalf of MetLife and other corporate customers. The Bank receives documents through the mail, among them checks from employers and accompanying remittance slips.

The Bank was recently advised that an unencrypted back-up tape containing images of these documents and other items that the Bank processed during the period February 25 to April 25, 2008, was lost while being transported by an outside carrier from the Bank's processing site in Philadelphia, PA to its data storage site in Pittsburgh, PA. The images may include personal information about you, such as name, address and social security number. Please bear in mind that these were images and not the original documents themselves.

Based on our investigation and information available to date, it appears that the tape was lost in transit. We have no reason to believe that the tape was stolen, or that unauthorized persons have accessed any information on the tape. **Also, please be assured that this incident did not affect the deposit and crediting of your annuity payments.**

Safeguarding confidential customer data is a top priority at The Bank of New York Mellon. We are implementing additional security procedures to help ensure that an event such as this does not occur again.

As an added precaution to help detect any possible misuse, we are offering you credit report monitoring services for two years, at no cost. We have engaged ConsumerInfo.com, Inc., an Experian® Company, to provide you with their Triple AlertSM Credit Monitoring product. This includes daily monitoring of credit reports from three major consumer reporting companies (Equifax®, Experian® and TransUnion®), e-mail monitoring alerts of key changes to your credit reports and more.

Through Experian®, we are also offering, without charge, Identity Theft Insurance in the amount of \$25,000 through Virginia Surety Company, Inc. with no deductible. (Note: Due to New York state law restrictions, Identity Theft Insurance coverage cannot be offered to residents of New York. Daily monitoring of credit reports, however, is available to New York residents.)

The free credit monitoring service and Identity Theft Insurance must be activated within 90 days of the date of this letter. To enroll, you should call us, toll-free at 1-877-279-1093. Our customer service representatives are available Monday through Friday, between the hours of 8 a.m. and 8 p.m. ET and Saturday, between the hours of 9 a.m. and 4 p.m. ET. When you call, you will be provided an activation code. This code is only for your use. With the activation code, you may then enroll with our customer service representative. You may also enroll online at <http://partner.experiandirect.com/triplealert>.

You may also wish to place a credit or security freeze on your consumer credit files. A credit or security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. **However, using a credit or security freeze may delay your ability to obtain credit.** You may request that a freeze be placed on your consumer report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address on the next page.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
(800) 685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com
(888) 909-8872

The following information should be included when requesting a credit or security freeze (documentation for you and your spouse must be submitted when freezing a spouse's consumer report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request also should include a copy of a government issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The consumer reporting agency may charge a reasonable fee to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the consumer reporting company. If you place a credit or security freeze within 90 days of the date of this letter, the Bank of New York Mellon will cover the cost of the initial placement and one removal (whether a temporary or permanent removal) of a credit or security freeze even if you are not the victim of identity theft. Because credit or security freezes can be temporarily removed on more than one occasion, you may incur costs associated with having a credit or security freeze on your credit file that BNY Mellon will not cover. Additional details on the credit or security freeze process, and how you may have BNY Mellon cover the charges, will be provided when you call the toll-free number below.

In all events, we recommend that you remain vigilant and take measures to regularly review and monitor your financial accounts to determine if there are any unauthorized transactions. If you detect any unauthorized transactions, promptly notify your financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities and to the Federal Trade Commission. You can learn more about how to protect yourself from becoming a victim of identity theft at the FTC's website: www.ftc.gov/bcp/edu/microsites/idtheft/index.html.

In addition, we recommend that you obtain a copy of your credit report from one or more of the national credit reporting companies. You may receive a free credit report once every 12 months through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling, toll-free to 877-322-8228, or by calling one of the three national credit reporting companies, toll free: Experian® at 888-397-3742; Equifax® at 800-685-1111; and TransUnion® at 800-916-8800.

You may also wish to place a "fraud alert" on your consumer credit files by contacting any of the three nationwide consumer reporting companies. A fraud alert means that creditors should take additional steps to verify the identity of anyone who applies for credit in your name, and should also reduce the possibility of identity theft. There is no charge for placing a fraud alert on your consumer credit files. You may place a fraud alert by contacting any of the credit reporting companies using the information provided above.

If you would like additional information or further assistance regarding this matter, please call us, toll-free at 1-877-279-1093.

We sincerely regret any inconvenience or concern this matter may have caused you.

Sincerely,

The Bank of New York Mellon

EXHIBIT C

BNY MELLON SHAREOWNER SERVICES
Attn: SHAREOWNER SERVICES
PO BOX 1690
Manchester, CT 06045



BNY MELLON
SHAREOWNER SERVICES

1-866-926-9805

THOMAS CARROLL HAMMOND
2700 GLENROSE ST
AUBURN HILLS
MI 48326

May 27, 2008

Dear Sir or Madam:

BNY Mellon Shareowner Services provides stock transfer agency, employee plan administration and related services for issuers of securities such as publicly traded corporations. While we have no reason to believe your information has been or will be accessed or misused, we are writing to inform you of an incident involving your personal information that we maintain in connection with these services. On February 27, 2008, our archive services vendor notified us that they could not account for one of several boxes of data backup tapes that they were transporting to an off-site storage facility. The missing tapes contained certain personal information, such as your name, address, Social Security number and/or shareowner account information, that we maintain in providing these services.

Although we have no indication of any improper access to this data, as a precaution, to help you detect any possible misuse of your data, we are offering you free credit monitoring for a 12-month period. We have engaged ConsumerInfo.com, Inc., an Experian® Company, to provide you with their Triple AlertSM Credit Monitoring product, which includes daily monitoring of your credit reports from three national credit reporting companies (Experian, Equifax® and TransUnion®), email monitoring alerts of key changes to your credit reports, and more.

For more information, please visit our website at <http://www.bnymellon.com/tapequery>. You have 90 days from the date of this notice to activate the credit monitoring by using the activation code [REDACTED]. This code is unique for your use and should not be shared. To learn more about Triple AlertSM and to enroll, go to <http://partner.consumerinfo.com/monitor> and follow the instructions. To enroll by phone, or if you have any questions, please call us toll-free at 1-877-278-3458. Our customer service representatives are available Monday through Friday, between 8 a.m. and 8 p.m. ET; and Saturday, between 9 a.m. and 4 p.m. ET.

We recommend that you regularly review statements from your accounts and obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by visiting <http://www.annualcreditreport.com> or by calling one of the three national credit reporting companies, toll-free: Experian at (888) 397-3742; TransUnion at (800) 916-8800; Equifax at (800) 685-1111. We recommend you remain vigilant and that you report any suspected identity theft to us and to proper law enforcement authorities, including the Federal Trade Commission. Please visit the FTC's web site, <http://www.ftc.gov/bcp/edu/microsites/idtheft>, to learn more about protecting yourself from identity theft, such as requesting a fraud alert.

Please be assured that we take the protection of your information very seriously and have taken additional measures to protect your account with us. We have implemented additional measures that will help prevent a similar occurrence. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

BNY Mellon Shareowner Services